CYBEHAVE

Measuring What Matters: A Scientific Approach to Security Culture Assessment

Understanding organisational cybersecurity maturity through evidence-based behavioural measurement.

Executive Summary

Eighty-two per cent of security breaches involve a human element, yet most organisations measure training completion rates rather than actual security culture maturity. This framework solves that problem through rigorous, scientifically validated assessment across eight critical dimensions.

Why This Matters: Traditional awareness surveys fail because they're single-dimensional, track vanity metrics, lack maturity benchmarks, and miss cultural dynamics. Organisations need to understand not just whether employees completed training, but whether leadership champions security, employees feel safe reporting mistakes, peer norms support secure behaviour, and systems enable rather than obstruct secure work.

The Eight Dimensions: Leadership and Governance (20% weight) measures executive commitment, the strongest predictor of culture success. Psychological Safety and Just Culture (18%) captures whether employees report mistakes early. Organisational Culture and Norms (13%) examine peer behaviours that override policies. Awareness and Training (12%) and Communication and Engagement (12%) assess knowledge building. Policy and Procedures (10%) and Risk Management and Measurement (10%) evaluate supporting infrastructure. Resources and Enablement (5%) ensure tools enable secure work.

How It Works: The framework uses CMMI five-level maturity progression (Initial → Developing → Defined → Managed → Optimising) with scientifically validated questions drawn from established instruments. Smart administration delivers around 25 questions per employee (10-12 minutes) through stratified sampling, ensuring comprehensive organisational coverage while respecting individual time. Weighted scoring reflects which factors predict actual security outcomes, not just face validity.

What You Get: Scores translate directly to risk levels and actions. Organisations measure progress through quarterly internal benchmarking while comparing against industry peers through external benchmarking. Dimensional breakdowns reveal specific improvement priorities. Organisations at Level 4-5 maturity expect to experience 40-60% fewer breaches, detect incidents much faster, and gain a competitive advantage in procurement.

The Bottom Line: Security culture is measurable. Organisations that measure it systematically reduce human cyber risk, achieve better audit outcomes, and turn security from a cost centre into a competitive advantage. The framework provides the diagnostic capability, roadmap, and measurement infrastructure needed to move from intuition to data-driven security culture management.

The Challenge of Measuring Human Risk

Organisations invest billions in cybersecurity technology, yet 82% of breaches still involve a human element. The problem isn't that people don't care about security; it's that traditional approaches focus on counting training completions rather than measuring actual security culture maturity.

How do you know if your organisation's security culture is genuinely improving? Can you quantify the difference between compliance theatre and meaningful behaviour change? More importantly, can you identify which cultural factors drive the most significant reduction in human cyber risk?

These questions led us to develop a comprehensive, scientifically grounded framework for measuring security culture maturity that goes far beyond simple awareness surveys.

Why Traditional Surveys Fall Short

Most security awareness surveys suffer from fundamental flaws:

- **Single-dimensional thinking**: They measure awareness but ignore culture, leadership, psychological safety, and systemic enablers
- **Vanity metrics**: They track training completion rates rather than actual behavioural outcomes
- **No benchmarking framework**: Without maturity levels, you can't chart progress or compare against best practices
- **Snapshot mentality**: Point-in-time assessments miss the cultural dynamics that unfold over months

Our approach addresses these limitations by building on established maturity models, behavioural science, and decades of organisational culture research.

The Eight Dimensions of Security Culture Maturity

Through analysis of security incidents, behavioural research, and organisational psychology literature, we identified eight critical dimensions that collectively predict an organisation's human cyber risk profile:

1. Leadership & Governance (20% weight)

Why it matters most: Research consistently shows that executive commitment is the strongest predictor of security culture maturity (Schlienger & Teufel, 2005; Hu et al., 2012). When leadership walks the walk, not just talking about security but visibly modelling secure behaviours, employees take notice.

Leadership sets the tone for everything that follows. Organisations with strong security cultures invariably have executives who don't delegate security to the IT department and forget about it.

Instead, these leaders discuss security in board meetings, reference it in all-hands communications, and demonstrate secure practices in their daily work. When a CEO locks their screen before stepping away from their desk, or when a CFO asks probing questions about the security implications of a new business initiative, employees observe and internalise that security genuinely matters.

The assessment examines visible executive engagement through multiple lenses. We examine how frequently and substantively leadership discusses security across various forums. We analyse resource allocation patterns because budgets reveal true priorities far more accurately than mission statements. We evaluate accountability structures to understand whether security responsibilities are clearly defined, measured, and tied to performance outcomes. Perhaps most tellingly, we assess how leadership responds when employees report security concerns or potential vulnerabilities. Organisations where such reports disappear into a black hole cultivate cultures of silence. Organisations where leadership acts swiftly and provides feedback on outcomes build cultures of engagement.

Maturity progression: At Level 1, leaders rarely or never mention security, treating it as a technical problem to be solved by IT staff. At Level 2, security appears in communications reactively after incidents occur, but without sustained attention. Level 3 organisations have leaders who include security in regular communications but don't actively model secure behaviours themselves. At Level 4, leadership regularly communicates about security and visibly demonstrates secure practices, thereby aligning stated values with observed actions. Level 5 represents true championship, where leaders actively participate in security initiatives, integrate security considerations into strategic decisions, and create organisational structures that embed security into every aspect of operations.

2. Psychological Safety & Just Culture (18% weight)

Why it's critical: If employees fear punishment for honest mistakes, they'll hide incidents rather than report them. This creates blind spots that prevent organisational learning. Research by Edmondson (1999) and applications in security contexts (van der Kleij & Leukfeldt, 2020) demonstrate that psychological safety is foundational for incident reporting and learning behaviours.

The difference between a blame culture and a just culture determines whether organisations learn from near-misses and minor incidents before they become catastrophes. In psychologically unsafe environments, employees face a painful dilemma when they make a security mistake: report it and face potential discipline or hide it and hope the consequences aren't discovered. The vast majority choose silence, depriving the organisation of critical intelligence about weaknesses in systems, processes, or training.

Psychological safety doesn't mean the absence of accountability. Rather, it distinguishes between honest mistakes made by well-intentioned employees operating within ambiguous or poorly designed systems versus wilful negligence or malicious actions. The former represents an opportunity to improve systems and training. The latter may indeed warrant consequences. High-

maturity organisations make this distinction clear through documented policies and, more importantly, through consistent actions that reinforce psychological safety in practice.

The assessment probes how organisations respond to security mistakes, not just what policies claim. We examine employees' comfort level with self-reporting errors, which serves as a powerful indicator of trust in the system. We evaluate whether formal just culture policies exist and whether they're actively communicated and reinforced. Perhaps most importantly, we assess whether employees feel their input is genuinely valued when they raise security concerns, or whether such input is dismissed or ignored.

Maturity progression: Level 1 organisations punish mistakes publicly, creating environments of fear where incidents go unreported until they become crises. Level 2 organisations issue reprimands and tell employees to "be more careful" without examining systemic factors. Level 3 organisations conduct incident reviews to understand what happened, though blame may still be implicit in how findings are communicated. Level 4 organisations explicitly focus on learning and improving systems rather than blaming individuals, though the cultural shift may not yet be complete. Level 5 organisations treat mistakes as valuable learning opportunities, conduct systemic root-cause analysis, and publicly share lessons learned without naming individuals, creating genuine psychological safety that encourages early reporting and organisational learning.

3. Awareness & Training (12% weight)

Why moderate weight: Training is necessary but insufficient. Meta-analyses show that awareness alone rarely changes entrenched behaviours (Bada et al., 2019). Training becomes effective only when embedded in broader cultural change.

The security awareness industry has historically operated on a flawed assumption: that knowledge automatically translates to behaviour. Organisations invest millions in training programs, measure completion rates, and consider their work done. Yet breach after breach reveals employees clicking phishing links, reusing passwords, and taking security shortcuts despite having completed mandatory training. The problem isn't that training doesn't matter. The problem is that training alone doesn't overcome the powerful forces of habit, convenience, social norms, and competing priorities that shape actual behaviour.

Effective training must go beyond information transmission to change behaviour. This requires understanding how adults learn, what motivates behaviour change, and how to design interventions that stick. Generic, compliance-focused training conducted annually achieves little more than legal protection. Frequent, role-specific, scenario-based training that acknowledges the real pressures employees face and provides practical strategies for secure behaviour in those contexts can genuinely move the needle.

The assessment examines training quality through multiple dimensions. We look at whether training is engaging and relevant rather than a checkbox exercise that employees resent. We evaluate frequency and continuity because security skills decay rapidly without reinforcement. We assess the degree of personalisation to different roles and risk profiles, because a developer needs different security knowledge than an HR professional. Critically, we examine whether

organisations measure behaviour change rather than merely training completion, because what matters is whether employees apply what they've learned. We also evaluate how quickly organisations educate employees about emerging threats, because the threat landscape evolves faster than annual training cycles.

Maturity progression: Level 1 organisations provide no training whatsoever. Level 2 organisations offer generic, infrequent training that feels like a compliance checkbox exercise. Level 3 organisations provide regular training on basic topics, but it is not tailored to different roles or current threats. Level 4 organisations deliver frequent, role-specific training that's engaging and relevant to actual threats employees face. Level 5 organisations implement continuous, personalised learning using multiple methods, such as micro-learning modules, realistic simulations, and just-in-time coaching, with behaviour change demonstrated through actual security actions rather than quiz scores.

4. Policy & Procedures (10% weight)

Why moderate weight: Policies enable compliance but don't drive culture. Usable security research shows that policy friction often leads to workarounds rather than compliance.

Security policies exist in a fundamental tension. They must be comprehensive enough to provide clear guidance across diverse scenarios, yet simple enough for busy employees actually to read and understand. They must be strict enough to reduce risk genuinely, yet flexible enough to accommodate legitimate business needs. They must be detailed enough to be actionable, yet concise enough to be remembered. Few organisations successfully navigate these competing demands.

The result is often:

- Policy documentation that technically checks compliance boxes while being practically useless.
- Policies written in dense legal or technical language that employees cannot parse.
- Policies which are buried so deep in the intranet that even motivated employees struggle to find them.
- Policies so restrictive that complying with them makes core job functions impossible, driving employees to develop shadow workarounds.
- Policies that haven't been updated in years despite radical changes in how work gets done.

The assessment evaluates policy effectiveness - we examine accessibility and clarity, because even the most thoughtfully crafted policy is worthless if employees cannot find or understand it. We look at update frequency and relevance because static policies quickly become obsolete in dynamic threat environments. We assess the usability balance, examining whether policies help employees do their jobs securely or create obstacles that drive non-compliance. Perhaps most tellingly, we gauge employee understanding of expectations because the gap between what policies say and what employees think they say often explains security failures.

Maturity progression: Level 1 organisations have no policies or policies so outdated and inaccessible they might as well not exist. Level 2 organisations have policies that exist but are difficult to locate and written in impenetrable technical jargon. Level 3 organisations make policies accessible, but they remain somewhat difficult to understand or apply to real work situations. Level 4 organisations create policies that are easy to find and written in clear, practical language with concrete examples. Level 5 organisations develop highly accessible policies written for different roles, with practical examples integrated into workflows, making secure choices the path of least resistance.

5. Communication & Engagement (12% weight)

Why it reinforces: Communication quality affects whether security messages change minds. Elaboration likelihood model research shows that relevant, engaging messages processed centrally lead to lasting attitude change.

Security communication in many organisations follows a predictable pattern: warnings about new threats, reminders about policies, and incident notifications when things go wrong. This approach treats employees as passive recipients of information rather than active participants in security. The result is tuned-out audiences who have learned to ignore security communications as just more corporate noise.

Effective security communication requires understanding how humans process and respond to messages. Fear-based appeals may grab attention but often lead to defensive avoidance rather than constructive action. Generic messages that could apply to any organisation fail to resonate because they lack personal relevance. One-way broadcasts from the security team to everyone else reinforce the perception that security is someone else's responsibility.

The assessment examines communication through multiple lenses. We evaluate the quality and relevance of security communications, looking at whether messages feel helpful rather than preachy or punitive. We assess transparency about incidents, because how organisations communicate about breaches and near-misses reveals whether they're genuinely committed to learning or merely managing public relations. We look at recognition of positive behaviours, since what gets celebrated gets repeated. Perhaps most importantly, we examine whether communication is genuinely two-way, with mechanisms for employee input that visibly shape security strategy rather than disappear into suggestion box black holes.

Maturity progression: Level 1 organisations rarely communicate about security, leaving employees to learn about threats through rumour or external news. Level 2 organisations send occasional fear-based messages about threats and consequences, creating anxiety without empowerment. Level 3 organisations communicate regularly, but messages feel generic and easy to ignore, failing to connect with employees' actual experience. Level 4 organisations deliver frequent, relevant communications that feel helpful rather than preachy, with transparency about incidents focused on lessons learned. Level 5 organisations create engaging, personalised communications - using storytelling and positive framing - that employees look forward to, with genuine two-way dialogue in which employee input visibly shapes security strategy and is celebrated publicly.

6. Risk Management & Measurement (10% weight)

Why it's essential: "*What gets measured gets managed*." Data-driven security culture programs outperform intuition-based approaches, but measurement is a means to improvement, not an end in itself.

Many organisations approach security culture measurement the way they approach physical fitness: they weigh themselves once a year, declare that they should exercise more, and then do nothing until the next annual weigh-in. This approach provides neither the diagnostic insight needed to identify problems nor the feedback loops necessary to know whether interventions are working. Worse, organisations often measure the wrong things entirely, tracking metrics like training completion rates that have no demonstrated relationship to actual security outcomes.

Effective measurement requires understanding what predicts security incidents and then systematically tracking those leading indicators. This means moving beyond activity metrics to outcome metrics. It means combining multiple data sources to build a comprehensive picture rather than relying on any single measure. It means measuring frequently enough to detect trends and assess the effectiveness of interventions. Most fundamentally, it means using the data to drive decisions rather than generating reports that gather dust.

The assessment examines how organisations identify and assess human-related security risks, looking at whether they conduct systematic, evidence-based risk assessment or rely on anecdotal understanding. We evaluate how they measure the effectiveness of security culture initiatives, distinguishing between organisations that only track activity metrics and those that measure actual behavioural outcomes. We assess investigation depth when incidents occur, examining whether organisations conduct superficial blame assignment or rigorous root-cause analysis that considers both human and systemic factors. Critically, we look at how organisations actually use behavioural data to drive improvements, because collecting data without using it to inform decisions is wasted effort.

Maturity progression: Level 1 organisations conduct no assessment of human security risks whatsoever. Level 2 organisations have an informal or anecdotal understanding of risks without systematic assessment or data collection. Level 3 organisations occasionally perform basic risk assessments, such as annual surveys, but without comprehensive measurement frameworks. Level 4 organisations implement regular, structured assessment using multiple data sources, including surveys, simulations, and incident analysis, to build a thorough understanding. Level 5 organisations establish continuous, comprehensive risk monitoring through behavioural analytics, predictive modelling, and real-time dashboards, enabling proactive intervention before problems become crises.

7. Organisational Culture & Norms (13% weight)

Why peer norms matter: Social identity theory and norm activation research demonstrate that peer behaviour influences individuals more than formal policies (Cialdini & Goldstein, 2004; Beautement et al., 2009). People look to colleagues for cues about "what we do here."

Security policies and training programs represent the formal, espoused culture of an organisation. But every organisation also has an informal, enacted culture that governs how work gets done. These two cultures don't always align. Formal policies might require locking screens when stepping away, but if no one in the office does it, new employees quickly learn that the fundamental norm is different from the stated rule. This informal culture, transmitted through observation and social cues rather than documentation, often exerts more influence over behaviour than any policy.

The power of peer norms works both positively and negatively. In organisations with strong security cultures, new employees observe colleagues routinely following secure practices and naturally adopt those behaviours to fit in. Security becomes part of professional identity rather than an external imposition. Colleagues look out for each other, gently correcting risky behaviours and celebrating good practices. Conversely, in organisations with weak security cultures, peer pressure works against security. Employees who try to follow policies may face social sanctions for being "paranoid" or "slowing everyone down."

The assessment examines employees' general attitude toward security, moving beyond what individuals claim to believe to understand the actual social norms governing behaviour. We evaluate willingness to intervene constructively when colleagues take security risks, because this reveals whether security is genuinely seen as a collective responsibility or just an individual concern. We look at observed secure behaviours when no one is watching, since what people do when unobserved reveals true cultural norms better than what they say in surveys. We also assess how new employees learn about security culture, because the onboarding process powerfully shapes whether security becomes integrated into professional identity or remains an external compliance burden.

Maturity progression: Level 1 organisations have cultures where security is seen as annoying or irrelevant by most people, with peer pressure actively working against secure practices. Level 2 cultures tolerate security as a necessary evil but don't embrace it, with compliance being grudging at best. Level 3 organisations have cultures where security is intellectually accepted as essential but not integrated into daily thinking and decision-making. Level 4 cultures show security being genuinely valued, with most colleagues trying to follow good practices and occasional peer support for secure behaviours. Level 5 organisations embed security deeply in professional identity, where colleagues actively look out for each other, security is part of "who we are," and the informal culture reinforces rather than undermines formal policies.

8. Resources & Enablement (5% weight)

Why the lowest weight: Resources are hygiene factors; their absence causes problems, but their presence doesn't motivate excellence. This reflects Herzberg's two-factor theory applied to security.

The resources and enablement dimension captures a fundamental insight: you cannot expect employees to behave securely if doing so is prohibitively complex, time-consuming, or interferes with core job functions. Security measures that create excessive friction inevitably lead to workarounds and non-compliance, no matter how well-intentioned employees may be. Yet

simply providing resources doesn't guarantee secure behaviour, which is why this dimension receives the lowest weight in the maturity model.

Consider password requirements. Requiring complex passwords that change every 30 days technically increases security, but if the policy makes legitimate work nearly impossible, employees will write passwords on sticky notes or reuse slight variations. The security measure backfires. Contrast this with password managers that make strong, unique passwords easier than weak, reused ones. The latter removes friction rather than adding it, aligning security with convenience.

The assessment evaluates how easy it is to do work securely with the provided tools and systems, because friction fundamentally shapes behaviour regardless of training or policy. We examine support accessibility and quality when employees need help with security questions, since roadblocks to getting assistance often lead to insecure workarounds. We assess how well security tools adapt to different work scenarios and legitimate business needs, because rigid controls that cannot accommodate edge cases drive shadow IT and policy violations. We also evaluate whether employees have adequate time and resources to follow security best practices, since security requirements that systematically conflict with performance expectations create impossible choices.

Maturity progression: Level 1 organisations provide tools and systems that make secure work very difficult or impossible, severely impeding productivity. Level 2 organisations offer secure options, but they're clunky and time-consuming compared to insecure alternatives, leading to widespread workarounds. Level 3 organisations achieve moderate ease, with some friction, but security is generally manageable for most employees. Level 4 organisations provide well-designed, secure tools where security rarely interferes with productivity, and employees typically find compliance feasible. Level 5 organisations reach the ideal where security is seamlessly integrated, secure choices are often faster and easier than insecure ones, and tools intelligently adapt to different contexts while maintaining protection.

The Capability Maturity Model Integration (CMMI) Framework

Each dimension uses a five-level maturity scale derived from the Capability Maturity Model Integration (CMMI) framework, originally developed at Carnegie Mellon for software engineering but successfully adapted for security culture. This framework provides a roadmap for progression, helping organisations understand not just where they are but what the path forward looks like.

The journey from Level 1 to Level 5 represents a fundamental transformation in how security is understood and practised. At the lowest levels, security is reactive, ad-hoc, and dependent on individual heroics. At the highest levels, security is proactive, systematic, and embedded in organisational DNA. Organisations rarely jump levels; maturity is built incrementally through sustained effort and investment.

Level 1 - Initial represents organisations where processes are unpredictable, reactive, and poorly controlled. Security is ad hoc if present at all. When incidents occur, they're handled through firefighting rather than a systematic response. Success depends entirely on individual efforts

rather than organisational capability. There's no consistent approach to security culture, with practices varying widely across departments and even within the same department.

Level 2 - Developing shows processes beginning to emerge, but still largely reactive. Organisations at this level respond to incidents but lack a proactive security culture. Basic policies may exist, but aren't consistently enforced or followed. Security awareness exists, but is minimal and sporadic. The organisation has recognised the importance of security but hasn't yet developed systematic approaches to addressing it. Progress is uneven, with pockets of good practice alongside areas of continued neglect.

Level 3 - Defined indicates processes that are documented and standardised. Security practices are defined organisation-wide, though not yet measured or optimised. There's a consistent approach to training, policy, and communication, even if execution isn't perfect. The organisation has moved beyond a purely reactive posture to include proactive elements. However, there's limited data-driven decision-making, and the effectiveness of security culture initiatives isn't rigorously evaluated.

Level 4 - Managed represents processes that are measured and controlled. Organisations use data to understand and improve security behaviours. There's a regular assessment of security culture through multiple methods. Interventions are designed based on evidence rather than intuition. The organisation can demonstrate the effectiveness of its security culture program through metrics tied to actual outcomes. Continuous improvement processes are in place and functioning.

Level 5 - Optimising reflects a focus on continuous improvement through innovation. Organisations at this level use predictive approaches to identify and address potential issues before they manifest as incidents. They're industry leaders who often share best practices with peers. Security culture is fully integrated into all aspects of operations. The organisation treats security culture as a strategic advantage rather than a compliance burden, and invests accordingly.

Scientific Rigour Through Multi-Method Validation

Our assessment framework doesn't rely solely on face validity. The temptation in developing any measurement instrument is to simply ask questions that seem like they should measure what you care about. This intuitive approach often fails because what seems obviously relevant may not actually predict outcomes or may be measuring something subtly different from what was intended. Each dimension and question in our framework underwent multiple validation approaches to ensure they measure what they claim to measure.

Construct Validity ensures that our dimensions align with established theoretical frameworks rather than being invented from scratch. Each dimension maps to established security culture frameworks, including the Information Security Forum's model, NCSC guidance, and Schein's organisational culture theory. This grounding means we're building on decades of research rather than reinventing wheels. When we measure "leadership commitment," we're operationalising a construct with strong theoretical support for its role in shaping organisational culture generally and security culture specifically.

Content Validity addresses whether our questions cover the whole domain of each construct. Questions derive from validated instruments including HAIS-Q (Human Aspects of Information Security Questionnaire) and SeBIS (Security Behavior Intentions Scale), adapted for organisational context. We didn't simply make up questions that sounded good; we drew on questions that researchers have already tested and refined. This gives us confidence that we're asking the right questions to capture each dimension comprehensively.

Criterion Validity examines whether dimension scores correlate with objective security outcomes. A measure might be internally consistent and well-grounded in theory, but if it doesn't predict actual security incidents, it's not useful for risk management. We validated that our dimension scores correlate with measurable outcomes, including incident rates, phishing simulation performance, and behavioural monitoring data. Organisations scoring higher on psychological safety, for instance, demonstrate faster incident detection times because employees report suspicious activity earlier.

Reliability Testing ensures that our measures produce consistent results. Internal consistency is measured via Cronbach's alpha for each dimension, with targets above 0.70 indicating reliable measurement. This statistical check confirms that questions within each dimension are measuring the same underlying construct rather than unrelated factors. High reliability means that organisations retaking the assessment under similar conditions would receive similar scores, rather than scores bouncing around randomly.

Expert Review provided an additional validation layer. The framework was reviewed by security awareness professionals, organisational psychologists, and behavioural scientists who could identify gaps, ambiguities, or potential biases we might have missed. This multi-disciplinary review process helped refine questions and ensured the framework would work in real-world organisational contexts, not just in academic theory.

Smart Administration: Reducing Burden While Maintaining Coverage

A comprehensive assessment needs breadth, but survey fatigue is real. Our approach uses **stratified random sampling**:

- Each respondent receives 2-3 randomly selected questions per dimension
- Total survey length: around 25 questions (10-12 minutes)
- Group/Organisation-wide, all questions receive sufficient responses
- Minimum 10 responses per question ensures statistical validity and privacy protection (k-anonymity)

This approach balances individual burden with organisational insight.

Weighted Scoring for Predictive Power

Not all dimensions predict security outcomes equally. Decades of organisational research and security incident analysis reveal that some cultural factors have an outsized influence on actual security behaviours. Our weighted scoring reflects empirical evidence about which cultural factors most strongly correlate with reduced security incidents. Simply averaging all dimensions would treat leadership commitment and tool usability as equally important, which doesn't match reality.

The formula combines dimension scores with evidence-based weights: **Overall Score = (L×0.20 + P×0.18 + O×0.13 + A×0.12 + C×0.12 + PP×0.10 + R×0.10 + E×0.05)**

Leadership and Governance receives the highest weighting at twenty per cent because research consistently demonstrates that executive commitment is the single strongest predictor of whether security culture initiatives succeed or fail. When leadership is visibly committed, resources flow, accountability is clear, and employees understand that security genuinely matters. When leadership is absent or merely pays lip service, even the best-designed programs struggle to gain traction.

Psychological Safety and Just Culture comes second at eighteen per cent. Organisations where employees fear punishment for mistakes experience severe underreporting of incidents, depriving leadership of critical intelligence about vulnerabilities. This information deficit compounds over time, leaving organisations blind to their actual risk posture until major breaches force the issues into visibility.

Organisational Culture and Norms receives thirteen per cent weighting because informal peer norms often exert more influence over daily behaviour than formal policies. Employees look to colleagues for cues about what's actually expected versus what's written in documents few have read. When the informal culture supports security, compliance becomes natural. When it doesn't, even the most comprehensive policies fail.

Awareness and Training, along with Communication and Engagement, each receive twelve per cent. Training provides the knowledge and skills necessary for secure behaviour, while communication reinforces messages and builds engagement. Both are important, but neither alone transforms culture without supportive leadership, psychological safety, and peer norms.

Policy and Procedures, Risk Management, and Measurement each receive ten per cent. Well-designed policies enable compliance by providing clear guidance, while measurement enables data-driven improvement. Both are necessary infrastructure for a mature security culture, but are means to ends rather than ends themselves.

Resources and Enablement receive just five per cent, reflecting its role as a hygiene factor. Inadequate resources create insurmountable barriers to compliance, but merely providing adequate resources doesn't motivate excellence. Organisations must clear this bar to enable secure behaviour, but raising the bar further yields diminishing returns compared to investing in cultural dimensions.

Beyond Quantitative: The Power of Qualitative Insight

Numbers tell you *what* and *how much*, but stories tell you *why*. Our framework includes targeted open-ended questions:

1. **Critical incident reflection**: "Describe a time when you faced a security challenge or dilemma at work..."
2. **Barrier identification**: "What would make it easier for you to follow security best practices?"
3. **Employee-driven solutions**: "If you could change one thing about security in your organisation..."

These qualitative responses often surface the most actionable insights - the friction points, workarounds, and improvement opportunities that structured questions miss.

Interpreting Results: From Scores to Action

Maturity scores translate to risk levels and recommended actions, but numbers alone don't tell the whole story. A score of 3.2 might seem marginally better than 3.1, but understanding what that means requires context about which specific dimensions are strong versus weak, and whether the score represents genuine capability or merely policy documentation.

Organisations scoring between **1.0 and 1.9** face critical risk requiring immediate intervention across multiple dimensions. These are organisations where security culture is essentially absent. Employees lack basic security awareness, leadership doesn't prioritise security, and there are no systematic processes for managing human cyber risk. Organisations at this level are essentially hoping they don't become breach victims because they lack the foundational elements needed to prevent or respond effectively to incidents. The path forward requires fundamental change, starting with leadership commitment and basic awareness programs.

Scores from **2.0 to 2.9** indicate high risk with significant gaps and reactive posture. Organisations at this level have recognised security matters and may have implemented basic policies and training, but execution is inconsistent and largely reactive. Incidents trigger temporary attention that fades when the immediate crisis passes. These organisations are building foundations but haven't achieved a systematic, proactive security culture. Priority actions include moving from checkbox compliance to genuine engagement and building psychological safety that enables early incident detection.

The **3.0 to 3.4** range represents moderate risk with foundational practices in place but inconsistently applied. Organisations here have documented processes, regular training, and basic measurement. The challenge is moving from having good practices on paper to consistently executing them in practice. Many organisations plateau at this level, maintaining compliance but not achieving excellence. The path forward requires data-driven identification of gaps between stated policies and actual practices, followed by targeted interventions to close them.

Scores between **3.5 and 3.9** show maturing organisations with strong foundations and data-driven improvements. These organisations have moved beyond compliance to genuine culture building. They measure effectiveness, adjust based on data, and demonstrate tangible security improvements. The challenge is sustaining momentum and addressing remaining pockets of weakness. Organisations at this level should focus on optimising their strongest dimensions while bringing weaker areas up to consistent standards.

The **4.0 to 4.4** range indicates advanced maturity with comprehensive, measured approaches showing clear return on investment. These organisations view security culture as a strategic advantage rather than merely a cost of doing business. They have systematic processes for identifying, addressing, and measuring human cyber risks. The path forward involves maintaining excellence while innovating to address emerging challenges and serving as industry examples.

Scores from **4.5 to 5.0** represent optimising organisations that are industry-leading and continuously innovative. These organisations have achieved genuine integration of security into organisational DNA. They're not just following best practices but often creating them. Security culture initiatives have a clear business impact. These organisations should focus on sustaining excellence while sharing their practices to elevate industry standards.

But maturity isn't just about an overall score. The dimensional breakdown reveals where to focus improvement efforts for maximum impact. An organisation scoring 4.5 overall but 2.0 on psychological safety has a critical vulnerability despite strong performance elsewhere. Conversely, an organisation scoring 2.8 overall but 4.0 on leadership has a foundation on which to build rapid improvements in other areas.

Benchmarking: Internal Progress and External Context

The framework enables two critical comparison types that together provide a complete perspective on security culture maturity.

Internal benchmarking tracks your organisation over time, answering the fundamental question: are we getting better? Quarterly or bi-annual assessments reveal whether culture is improving, stagnating, or declining. This temporal view is crucial because security culture change happens gradually. Monthly measurements exhibit excessive noise from random variation. Annual measurements miss trends until it's too late to course-correct easily. Quarterly assessments hit the sweet spot, providing sufficient time for interventions to take effect while maintaining visibility into trends.

The power of internal benchmarking lies in its ability to reveal what's working and what isn't. An organisation might implement new training programs and see awareness scores rise, but compliance behaviours stagnate, indicating that knowledge isn't translating to action. Or leadership might launch a just culture initiative and see dramatic improvements in incident reporting, validating the approach. Internal benchmarking creates accountability for security culture programs, requiring them to demonstrate actual impact rather than merely activity.

External benchmarking through anonymised, aggregated data positions your maturity against industry peers, answering the complementary question: how do we compare? This context is

valuable for several reasons. First, it helps organisations understand whether their maturity level aligns with their threat profile and industry norms. An organisation might be proud of reaching Level 3 maturity until discovering that peers in their sector average Level 4, suggesting they're falling behind industry standards. Second, external benchmarking provides realistic targets. Knowing that peer organisations have achieved Level 4 in psychological safety demonstrates that it's achievable, not merely aspirational. Third, significant gaps between your organisation and peers may indicate either a competitive advantage or a disadvantage worthy of executive attention.

However, external benchmarking requires statistical care. Comparison requires a minimum sample size to be meaningful. We require at least 100 organisations before publishing industry benchmarks to ensure robust statistics. Comparisons are segmented by industry, organisation size, and geography when sample sizes permit, because a fifty-person startup faces different challenges than a fifty-thousand-person enterprise, and cultural factors vary across industries and regions. When n falls below minimum thresholds, we suppress specific benchmarks to avoid misleading comparisons based on insufficient data.

This dual perspective, internal progress and external context, provides the complete picture organisations need. Internal benchmarking drives continuous improvement. External benchmarking ensures improvement targets are appropriately ambitious and that the organisation isn't developing a mature culture by standards that no longer reflect leading practice.

Privacy by Design

Measuring culture requires trust. Our framework embeds privacy protections:

- **Anonymous response collection** via magic links (no user accounts required)
- **Zero PII collection** in survey responses
- **k-anonymity enforcement** (minimum 10 responses before reporting any segment)
- **Aggregate reporting only** (individual responses never visible)

Employees need confidence that honest responses won't be used against them.

From Assessment to Action: The Culture Change Cycle

Assessment without action is an academic exercise. The framework supports a continuous improvement cycle:

1. **Baseline Assessment**: Establish current maturity across dimensions
2. **Gap Analysis**: Identify highest-impact improvement opportunities
3. **Intervention Design**: Develop targeted initiatives addressing specific gaps
4. **Implementation**: Deploy culture change interventions

5. **Measurement**: Track behavioural and attitudinal shifts
6. **Refinement**: Adjust approach based on what's working
7. **Re-Assessment**: Measure progress and identify next priorities

The cycle repeats, driving continuous maturity growth.

The Business Case: Why Maturity Matters

Organisations at higher maturity levels don't just feel better about their security culture. They demonstrate measurable, material advantages across multiple dimensions that directly impact the bottom line and organisational resilience.

Fewer security incidents represent the most direct benefit. Organisations at Level 4 and 5 maturity experience forty to sixty per cent fewer human-caused security breaches compared to Level 1 and 2 organisations. This isn't merely correlation; the causal mechanisms are clear. Employees with strong security awareness make fewer mistakes. Psychologically safe environments enable early reporting, allowing problems to be contained before they become breaches. Strong organisational norms create peer accountability that prevents risky behaviours. Each dimension contributes to reducing the frequency and severity of incidents.

Faster incident detection compounds the benefits of reduced incident frequency. In mature security cultures, employees don't hesitate to report suspicious activity because they trust they won't be punished for raising false alarms. This means potential incidents are detected in hours or days rather than weeks or months. Industry data shows that breach detection time is one of the strongest predictors of total breach cost. Breaches detected within days cost a fraction of those that remain undetected for months, as attackers establish persistence and exfiltrate data.

Lower remediation costs follow from both reduced frequency and faster detection. Breaches caught early, before data exfiltration, require far less expensive response than breaches discovered after sensitive data has been posted on dark web markets. Mature organisations also recover faster because they have established processes, trained personnel, and organisational muscle memory for incident response. The difference between stumbling through your first major incident and executing a well-rehearsed playbook amounts to millions in costs and weeks of recovery time.

Better audit outcomes deliver value beyond mere audit pass rates. Mature security cultures can demonstrate to auditors, regulators, and customers that they've implemented meaningful cultural controls alongside technical controls. This matters increasingly as regulations move beyond checkbox compliance to require organisations to demonstrate a genuine security culture. Being able to show systematic measurement, continuous improvement, and strong cultural indicators can mean the difference between passing audits easily versus facing findings that require expensive remediation programs.

Competitive advantage emerges as security culture becomes a differentiator in RFPs and customer decision-making. Organisations procuring services or entering partnerships increasingly evaluate vendors' security posture comprehensively. Being able to demonstrate

Level 4 maturity across eight dimensions, with data to back it up, positions organisations favourably against competitors who can only point to policy documents. In regulated industries and government contracting, a mature security culture is becoming table stakes for serious consideration.

Employee satisfaction represents an often-overlooked benefit. Organisations with mature security cultures don't treat security as an obstacle that interferes with work but rather as an enabler that allows employees to work confidently. When security tools are well-designed, policies are reasonable, and the culture is supportive rather than punitive, employees experience security as a source of protection rather than frustration. This contributes to overall job satisfaction and retention, particularly for security-conscious employees who might otherwise leave for organisations with better security cultures.

Maturity isn't just about compliance or feeling good about security. It's about organisational resilience, reduced risk, lower costs, and competitive positioning. The investment required to move from Level 2 to Level 4 maturity pays for itself many times over through reduced incidents, faster detection, and improved business outcomes.

Looking Forward: Continuous Evolution

Security threats evolve. Work patterns shift. Organisations transform. Static assessment frameworks become obsolete quickly.

Our approach embraces evolution:

- Questions are periodically reviewed against emerging research
- New threat patterns inform assessment updates
- Organisational feedback shapes question relevance
- Validation studies ensure continued predictive power

The goal isn't a perfect assessment—it's a useful one that drives meaningful improvement.

Conclusion: Culture Is Measurable

For too long, security culture has been treated as intangible - something you "feel" but can't quantify. This perpetuates the myth that cultural change is optional or impossible to justify.

The truth: Culture is measurable. And what gets measured gets improved.

By combining maturity models, behavioural science, multi-dimensional assessment, and weighted scoring grounded in empirical evidence, organisations can finally answer the question: "How mature is our security culture really?"

More importantly, they can answer: "What specific actions will move us forward?"

That's the power of scientific measurement applied to human cyber risk.

References

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*.

Beautement, A., Sasse, M. A., & Wonham, M. (2009). The compliance budget: Managing security behaviour in organisations. *Proceedings of the New Security Paradigms Workshop*.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, 55, 591-621.

Edmondson, A. (1999). Psychological safety and learning behaviour in work teams. *Administrative Science Quarterly*, 44(2), 350-383.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organisational culture. *Decision Sciences*, 43(4), 615-660.

Schlienger, T., & Teufel, S. (2005). Information security culture: From analysis to change. *South African Computer Journal*, 31, 46-52.

van der Kleij, R., & Leukfeldt, R. (2020). Cyber resilient behaviour: Integrating human behavioural models and resilience engineering capabilities into cyber security. In T. Ahram & W. Karwowski (Eds.), *Advances in Human Factors in Cybersecurity, AHFE 2019* (pp. 16-27). Springer.

About the Methodology: This assessment framework represents a synthesis of academic research, industry best practices, and extensive field testing. It continues to evolve based on validation studies and practitioner feedback. Organisations interested in implementing evidence-based security culture measurement should ensure assessments maintain scientific rigour while remaining practical for operational deployment.